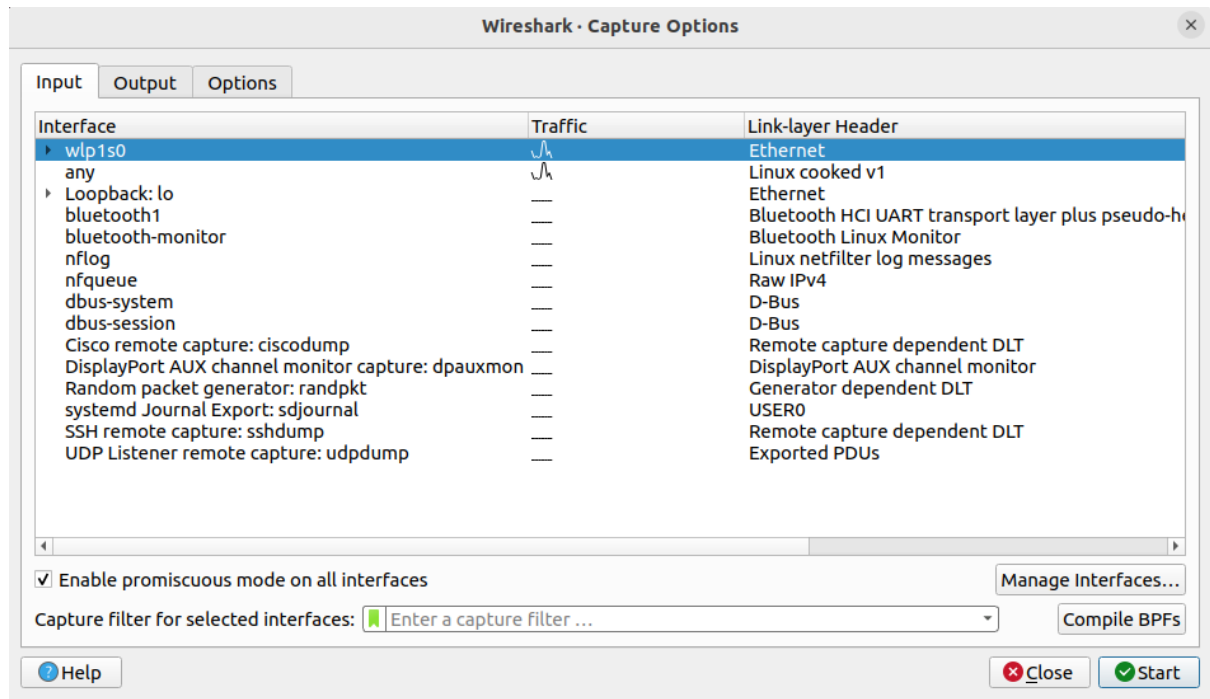


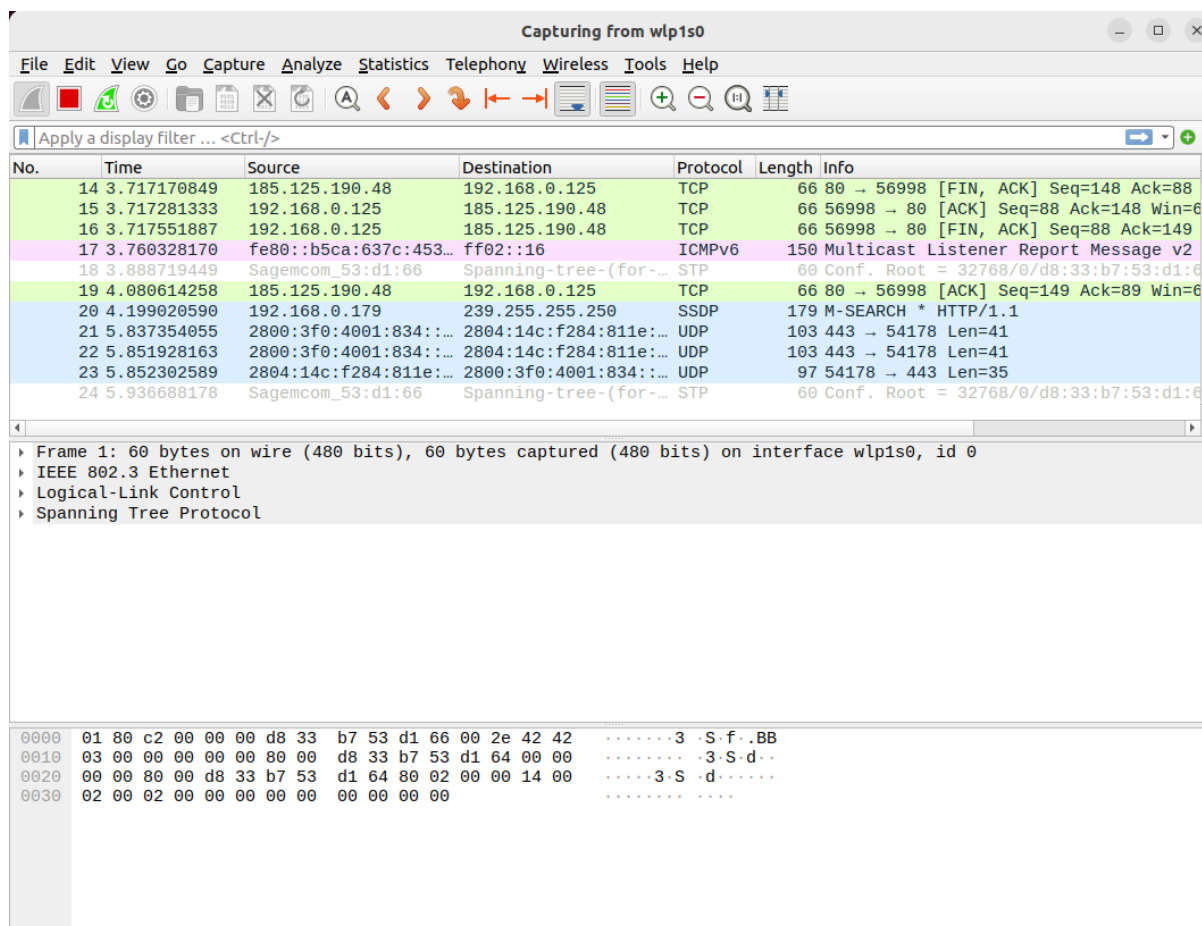
Aluno: Luís Eduardo Bertelli

Coleta de dados com Wireshark

1 - Selecionando a interface de rede apropriada:

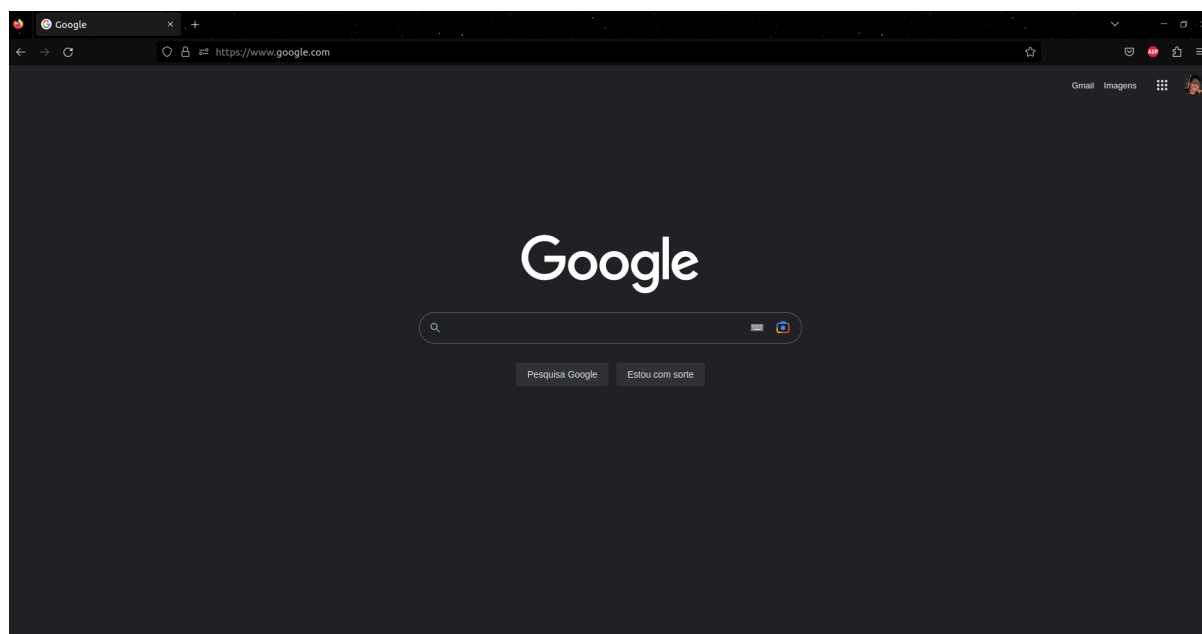


Como a intenção é monitorar o tráfego de rede, a interface escolhida que corresponde a conexão de rede que eu estou usando para me conectar à internet é “wlp1s0”, que é a interface para conexão wireless.



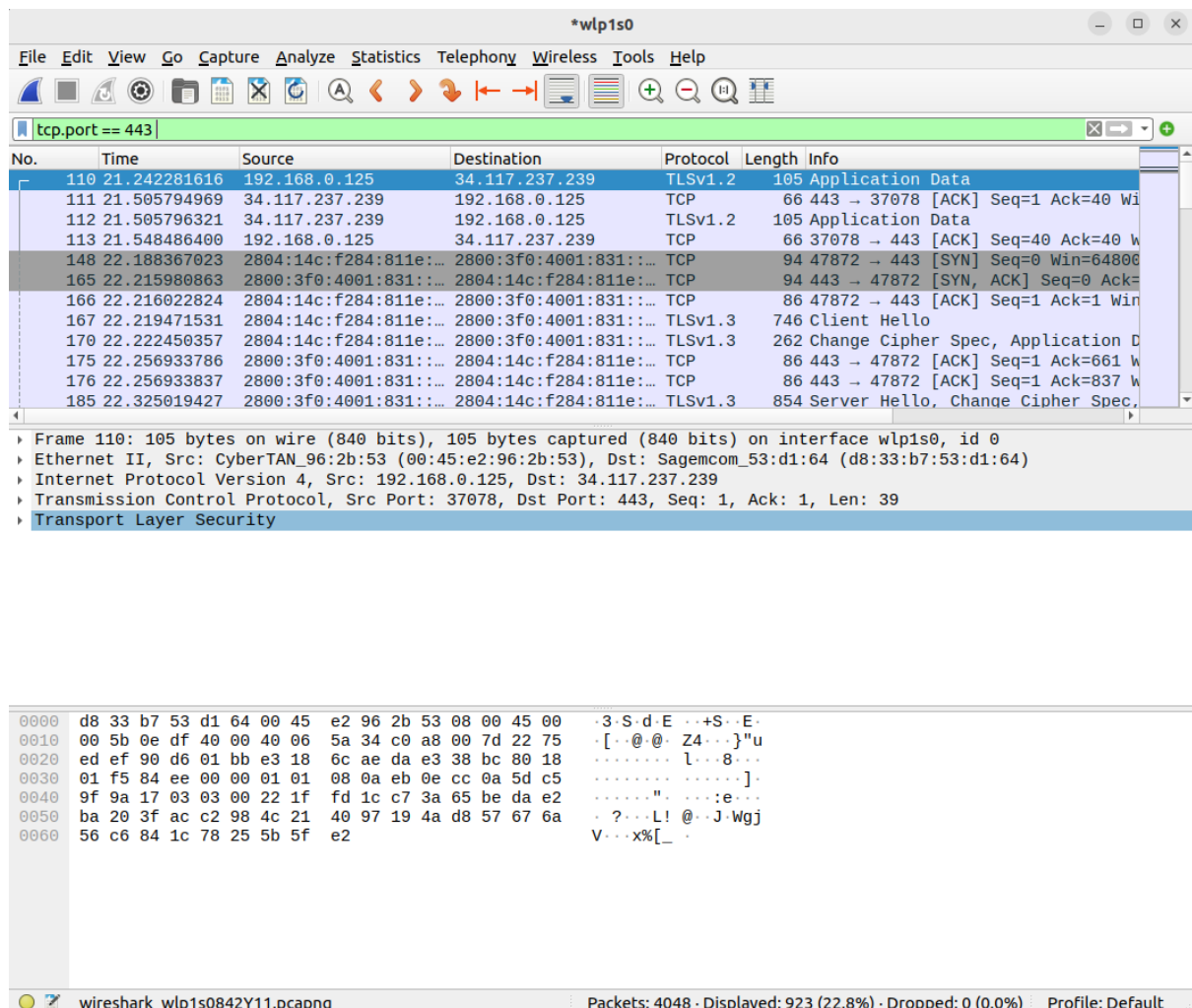
O programa já está recolhendo dados de tráfego.

2 - Acessando um endereço usando protocolo HTTPS.



O endereço escolhido para análise foi <https://www.google.com/>

3 - Aplicando filtro de porta para procurar dados no wireshark



Wireshark interface showing a packet capture on interface wlp1s0. The filter applied is `tcp.port == 443`. The packet list shows several packets, including TLSv1.2 and TCP. The packet details pane shows the structure of a TLSv1.2 packet, including Client Hello, Change Cipher Spec, and Server Hello. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Como o link acessado é um protocolo HTTPS, a porta utilizada será a porta 443, o filtro utilizado será `tcp.port == 443`, se o link fosse do protocolo HTTP, a porta utilizada seria 80.

4 - Encontrando IP do google

```
luis2535@luis2535-IdeaPad-3-15ALC6:~$ ping google.com
PING google.com(2800:3f0:4001:821::200e (2800:3f0:4001:821::200e)) 56 data bytes
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=1 ttl=54 time=102 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=2 ttl=54 time=125 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=3 ttl=54 time=45.3 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=4 ttl=54 time=67.9 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=5 ttl=54 time=90.6 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=6 ttl=54 time=113 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=7 ttl=54 time=136 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=8 ttl=54 time=55.9 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=9 ttl=54 time=79.4 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=10 ttl=54 time=102 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=11 ttl=54 time=125 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=12 ttl=54 time=45.4 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=13 ttl=54 time=68.4 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=14 ttl=54 time=90.7 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=15 ttl=54 time=114 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=16 ttl=54 time=35.0 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=17 ttl=54 time=34.6 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=18 ttl=54 time=79.8 ms
64 bytes from 2800:3f0:4001:821::200e (2800:3f0:4001:821::200e): icmp_seq=19 ttl=54 time=103 ms
```

Ao digitar ping google.com, conseguimos que o IP que será utilizado para identificar o google é o seguinte: 2800:3f0:4001:821::200e.

5 - Atividade do wireshark encerrada.

6 - Iniciar coleta de dados:

I - Protocolo de camada de transporte

No.	Time	Source	Destination	Protocol	Length	Info
165	22.215980863	2800:3f0:4001:831::...	2804:14c:f284:811e::...	TCP	94	443 → 47872 [SYN, ACK] Seq=0 Ack=...
166	22.216022824	2804:14c:f284:811e::...	2800:3f0:4001:831::...	TCP	86	47872 → 443 [ACK] Seq=1 Ack=1 Win=...
167	22.219471531	2804:14c:f284:811e::...	2800:3f0:4001:831::...	TLSv1.3	746	Client Hello
170	22.222450357	2804:14c:f284:811e::...	2800:3f0:4001:831::...	TLSv1.3	262	Change Cipher Spec, Application D...
175	22.256933786	2800:3f0:4001:831::...	2804:14c:f284:811e::...	TCP	86	443 → 47872 [ACK] Seq=1 Ack=661 W...
176	22.256933837	2800:3f0:4001:831::...	2804:14c:f284:811e::...	TCP	86	443 → 47872 [ACK] Seq=1 Ack=837 W...
185	22.325019427	2800:3f0:4001:831::...	2804:14c:f284:811e::...	TLSv1.3	854	Server Hello, Change Cipher Spec,
186	22.325019487	2800:3f0:4001:831::...	2804:14c:f284:811e::...	TLSv1.3	148	Application Data
187	22.325019557	2800:3f0:4001:831::...	2804:14c:f284:811e::...	TLSv1.3	117	Application Data
190	22.325080165	2804:14c:f284:811e::...	2800:3f0:4001:831::...	TCP	86	47872 → 443 [ACK] Seq=837 Ack=769...
191	22.325101065	2804:14c:f284:811e::...	2800:3f0:4001:831::...	TCP	86	47872 → 443 [ACK] Seq=837 Ack=831...

Analisando o pacote 175, que tem como fonte o ip da página do google, conseguimos as seguintes informações sobre o protocolo de camada de transporte.

Wireshark · Packet 175 · wlp1s0

▶ Frame 175: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlp1s0

▶ Ethernet II, Src: Sagemcom_53:d1:64 (d8:33:b7:53:d1:64), Dst: CyberTAN_96:2b:53 (00:45:e2:96:2b:53)

▶ Internet Protocol Version 6, Src: 2800:3f0:4001:831::200e, Dst: 2804:14c:f284:811e:d47f:...

▼ Transmission Control Protocol, Src Port: 443, Dst Port: 47872, Seq: 1, Ack: 661, Len: 0

Source Port: 443

Destination Port: 47872

[Stream index: 3]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2641786204

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 661 (relative ack number)

Acknowledgment number (raw): 1392586362

1000 = Header Length: 32 bytes (8)

0000	00 45 e2 96 2b 53 d8 33	b7 53 d1 64 86 dd 60 04	.E...S.3 .S.d...
0010	30 c5 00 20 06 36 28 00	03 f0 40 01 08 31 00 00	0... 6(. .@. 1..
0020	00 00 00 00 20 0e 28 04	01 4c f2 84 81 1e d4 7f(. .L....
0030	1a 38 88 9f 06 01 01 bb	bb 00 9d 76 75 5c 53 01	.8.....vu\S.
0040	2e 7a 80 10 01 06 5a 1e	00 00 01 01 08 0a af 89	.Z....Z.
0050	fc 72 99 97 d6 7e		.r....~

Help

Close

Aqui, conseguimos analisar que o protocolo é um Transmission Control Protocol(TCP) com porta de origem 443 e porta de destino 47872. Temos ainda a flag ACK e informações do tamanho do pacote e de seu tempo de vida util.

-Volume de dados trafegados

Ethernet · 40		IPv4 · 27		IPv6 · 42		TCP · 22		UDP · 108	
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.0.125	56998	185.125.190.48	80	9	844	5	425	0	0
192.168.0.125	37078	34.117.237.239	443	12	1.011	7	603	0	0
192.168.0.125	46710	34.111.73.144	443	13	1.119	8	697	0	0
192.168.0.125	33530	35.241.9.150	443	13	1.119	8	697	0	0
2804:14cf284:811e:d47f:1a38:889f:601	58882	2800:3f0:4001:829::2003	443	12	1.251	8	829	0	0
2804:14cf284:811e:d47f:1a38:889f:601	41420	2800:3f0:4001:833::200a	443	12	1.251	7	743	0	0
2804:14cf284:811e:d47f:1a38:889f:601	53600	2800:3f0:4001:834::200e	443	12	1.251	7	743	0	0
2804:14cf284:811e:d47f:1a38:889f:601	51964	2800:3f0:4001:82f::200e	443	13	1.337	8	829	0	0
2804:14cf284:811e:d47f:1a38:889f:601	39872	2600:1901:0:92a9::	443	13	1.379	8	857	0	0
2804:14cf284:811e:d47f:1a38:889f:601	46296	2800:3f0:4001:813::200e	443	14	1.423	8	829	0	0
2804:14cf284:811e:d47f:1a38:889f:601	41114	2800:3f0:4001:825::200a	443	14	1.459	8	853	0	0
2804:14cf284:811e:d47f:1a38:889f:601	38384	2800:3f0:4001:820::200e	443	16	1.607	9	915	0	0
2804:14cf284:811e:d47f:1a38:889f:601	55728	2800:3f0:4001:821::200a	443	16	1.607	9	915	0	0
2804:14cf284:811e:d47f:1a38:889f:601	57800	2600:1419:5c00::bd56:7a09	80	19	1.634	10	860	0	0
2804:14cf284:811e:d47f:1a38:889f:601	51012	2800:3f0:4001:82f::2004	443	17	3.289	9	1.732	0	0
2804:14cf284:811e:d47f:1a38:889f:601	47844	2800:3f0:4001:833::2002	443	24	4.056	13	2.163	0	0
192.168.0.125	40208	34.120.208.123	443	52	8.434	25	5.124	0	0
2804:14cf284:811e:d47f:1a38:889f:601	51374	2800:3f0:4001:813::200e	443	21	10 k	12	1.808	0	0
192.168.0.125	45986	34.120.115.102	443	29	13 k	16	1.423	0	0
2804:14cf284:811e:d47f:1a38:889f:601	33064	2800:3f0:4001:831::200e	443	63	24 k	31	18 k	0	0
2804:14cf284:811e:d47f:1a38:889f:601	47872	2800:3f0:4001:831::200e	443	66	27 k	34	21 k	0	0
2804:14cf284:811e:d47f:1a38:889f:601	44760	2800:3f0:4001:825::200a	443	491	134 k	188	62 k	0	0

Na barra de menu achamos a função 'statistics' e vamos na aba 'conversations', ai vamos na aba de interesse(TCP) e selecionamos uma linha que seja de nosso interesse, no campo bytes temos o volume de dados trafegados em uma sessão, aqueles que possuem o endereço como 2800:3f0:4001:821::200a estão relacionados ao google.

-MSS definido para conexão

*wlp1s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
3506	143.382443444	2804:14c:f284:811e::...	2800:3f0:4001:834::...	TLSv1.2	110	Application Data
3507	143.469846925	2800:3f0:4001:834::...	2804:14c:f284:811e::...	TCP	86	443 → 53600 [ACK] Seq=79 Ack=143
3508	143.469847466	2800:3f0:4001:834::...	2804:14c:f284:811e::...	TCP	86	443 → 53600 [FIN, ACK] Seq=79 Ack=143
3509	143.469933430	2804:14c:f284:811e::...	2800:3f0:4001:834::...	TCP	86	53600 → 443 [ACK] Seq=143 Ack=80
3512	144.382741749	2804:14c:f284:811e::...	2800:3f0:4001:821::...	TLSv1.2	125	Application Data
3513	144.383022475	2804:14c:f284:811e::...	2800:3f0:4001:821::...	TLSv1.2	110	Application Data
3514	144.383052428	2804:14c:f284:811e::...	2800:3f0:4001:821::...	TCP	86	55728 → 443 [FIN, ACK] Seq=142 Ack=143
3515	144.472521290	2804:14c:f284:811e::...	2800:3f0:4001:821::...	TCP	86	[TCP Retransmission] 55728 → 443
3516	144.476005647	2800:3f0:4001:821::...	2804:14c:f284:811e::...	TCP	86	443 → 55728 [ACK] Seq=79 Ack=142
3517	144.476006648	2800:3f0:4001:821::...	2804:14c:f284:811e::...	TCP	86	443 → 55728 [FIN, ACK] Seq=79 Ack=142
3518	144.476006668	2800:3f0:4001:821::...	2804:14c:f284:811e::...	TCP	86	443 → 55728 [ACK] Seq=80 Ack=143

Urgent Pointer: 0

- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - TCP Option - No-Operation (NOP)
 - Kind: No-Operation (1)
 - TCP Option - No-Operation (NOP)
 - Kind: No-Operation (1)
 - TCP Option - Timestamps: TSval 1129904899, TSecr 1144662372
 - Kind: Time Stamp Option (8)
 - Length: 10
 - Timestamp value: 1129904899
 - Timestamp echo reply: 1144662372
- [Timestamps]
 - [Time since first frame in this TCP stream: 111.463088953 seconds]

```

0000 00 45 e2 96 2b 53 d8 33 b7 53 d1 64 86 dd 60 01  .E..S.3.S.d...
0010 2b 9b 00 20 06 76 28 00 03 f0 40 01 08 21 00 00  +...v(. ..@..!..
0020 00 00 00 00 20 0a 28 04 01 4c f2 84 81 1e d4 7f  ....(. .L.....
0030 1a 38 88 9f 06 01 01 bb d9 b0 40 43 07 b4 4e 51  .8.....@C..NQ
0040 12 1f 80 11 01 0b 97 7b 00 00 01 01 08 0a 43 58  .....{ .....CX
0050 fb 03 44 3a 29 64  ..D:)d

```

Protocols carried by this frame (frame.protocols) Packets: 4048 · Displayed: 923 (22.8%) · Dropped: 0 (0.0%) Profile: Default

Para encontrar o MSS, vamos na parte de detalhes dos pacotes e procuramos o campo TCP Options, expandindo esse campo deveríamos achar o Maximum segment size(MSS), que é o valor que indica o tamanho máximo do segmento que a outra extremidade da conexão TCP pode receber em bytes, nos pacotes que eu pesquisei porém, essa opção não estava aparecendo, e pelas minhas pesquisas quando essa opção não aparece significa que o MSS é o padrão para um protocolo TCP/IP, no caso de 536 bytes.